414 Rec'd PCT/PTO 27 NOV 2000 PCT

FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 1242-00

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): 09/701456

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/26839	29 SEP 00	01 OCT 99

TITLE OF INVENTION
PORT BLOCKING METHOD AND SYSTEM

OIPE JC26 NOV 27 2000 PATENT & TRADEMARK OFFICE

APPLICANT(S) FOR DO/EO/US
FRIEDMAN, George; STAREK, Robert Phillip; MURDOCK, Carlos A.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☒ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ A copy of the International Search Report (PCT/ISA/210).
8. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☐ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

acknowledgement postcard

PCTUS1/REV03

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/701456	PCT/US00/26839	1242-00

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1,000.00**	
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO **$860.00**	
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**	
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**	
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	
	ENTER APPROPRIATE BASIC FEE AMOUNT =	**$710.00**
	Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	15 - 20 =	0	x $18.00	**$0.00**
Independent claims	10 - 3 =	7	x $80.00	**$560.00**
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**
	TOTAL OF ABOVE CALCULATIONS =			**$1,270.00**
☐	Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable).**			**$0.00**
	SUBTOTAL =			**$1,270.00**
	Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +			**$0.00**
	TOTAL NATIONAL FEE =			**$1,270.00**
☒	Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			**$40.00**
	TOTAL FEES ENCLOSED =			**$1,310.00**
				Amount to be: refunded $
				charged $

☒ A check in the amount of **$1,310.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **13-3405** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

PAUL A. TAUFER, ESQ.
SCHNADER HARRISON SEGAL & LEWIS, LLP
1600 MARKET STREET, SUITE 3600
PHILADELPHIA, PA 19103
(215) 751-2475
(215) 568-6946 (fax)

SIGNATURE

Paul A. Taufer
NAME

35,703
REGISTRATION NUMBER

November 27, 2000
DATE

09/701456
PCT/US00/26839
Rec'd PCT/PTO 27 NOV 2000

PORT BLOCKING METHOD AND SYSTEM

Field of the Invention:

The invention relates to the protection of data stored in a computer, and more particularly, to data which has been secured and opened by non-secure applications where a high level application or operating system component acts to disable certain system resources in order to protect the security of data.

Background of the Invention:

In computer systems, processes may access many system resources, such as serial ports or connections to the Internet. In a situation in which secured data is being accessed by a non-secured application, a means must be developed by which the non-secured application can be restricted from performing operations which might compromise the security of the data.

It is known to open secure data in a system which is completely isolated from outside communications, which has no connection to means by which an unsecured application may, by accident or sabotage, compromise the secured data. It is also known to open secure data with secure applications, which are known to be free from the risk of accident or sabotage that would compromise the secured data. These solutions prevent the use of popular software applications to open secured data, or the use of a computer which is not disconnected from outside communications, and thereby are limited in their usefulness.

Summary of the Invention:

The invention discloses a port blocking method particularly applicable to a system in which secured data is transmitted to a recipient computer for use with non-secured applications. An illustrative embodiment of the invention comprises performing a security check on a process and blocking calls for use of a port if they come from a process using secured data. The tracking of secured processes may include determining whether and how often a secured process should be allowed to use a port. The security check may include determining whether the process is secured by consulting a secured process list and determining whether the resource should be available to the process requesting use of the resource.

Further disclosed is a port blocking system, secured data transmission system using

port blocking, computer-readable medium programmed to block port use, and a computer configured to block port use.

Description of the Drawings:

The invention is best understood from the following detailed description when read with the accompanying figures.

Figure 1 is an schematic diagram of a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 2 is a flow chart of a port request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(a) is a flow chart of a port open request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(b) is a flow chart of a port close request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(c) is a flow chart of a security check in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Detailed Description of the Invention:

The invention disclosed prohibits certain processes from utilizing the port resources of the computer on which they are running. These may be secured processes for example, ones which have opened secure data. In a preferred embodiment of the invention, the status of a process as secured is determined by the processes presence on a list of secured processes.

In a preferred embodiment, as shown in Fig. 1, in a computer 100, a control application 110 runs on the kernel (ring 0) level 120 and applications 130 run on higher levels 140. When applications request access to port 150, control application 110 monitors and handles these access requests.

As shown in Fig. 2, in some computer systems, for example, Microsoft Windows NT and Windows 2000 operating systems, the port monitoring is able to intercept all port-related calls. When a port request is initiated 200, control application (110 in Fig. 1) intercepts that request, and determines the process id 210. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to open a port. The

process id is used to determine whether the process is secure (not allowed to open a port) 220. If it is secure, the request is blocked at 230. If it is not secure, then the request is passed on to the port 250.

As shown in Fig. 3(a), in some computer systems, for example, Microsoft Windows 95 and 98 operating systems, the port monitoring is able to intercept only open and close calls. In order to ensure that a process which has access to a port does not then become a secure process, a check must be performed on any process which is to become secure. When an open port request is initiated 300, control application (110 in Fig. 1) intercepts that request, and determines the process id 310. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to open a port. The process id is used to determine whether the process is secure (not allowed to open a port) 320. If it is secure, the request is blocked, 330, and the call is tracked 340. If it is not secure, then the request is passed on to the port and the process ID and port handle are tracked 350.

As shown in Fig. 3(b), when a close port request is initiated 360, control application (110 in Fig. 1) intercepts that request, and completes the call 362. Then the process ID and port handle is removed from the database of tracked open ports 364.

In addition to these operations on open port and close port requests, as shown in Fig. 3(c), when a process undergoes the security check which determines whether it will be secured, 370, its process id is checked against the database of tracked open ports 372. If the process has open ports, the process may not be made secure and the security check fails 374, and the security check is completed 376. If the process does not have open ports it will pass the security check and the process id will be added to the list of secured processes 378.

A further illustrative embodiment of the invention is directed to a port blocking system wherein certain processes are restricted from using a port, according to the methods provided herein. Further disclosed is a secured data transmission system having a port blocking component to prohibit certain processes from using a port according to the methods provided herein. Still further disclosed is a computer-readable medium programmed to block port use according to the methods provided herein. Still further disclosed is a computer configured to include a port blocking system to block certain processes from using a port according to the methods provided herein.

The terms "computer", "computer system", or "system" as used herein should be broadly construed to include any device capable of receiving, transmitting and/or using

information including, without limitation, a processor, microprocessor or similar device, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television, such as for example, a television adapted to be connected to the Internet or an electronic device adapted for use with a television, a cellular telephone, a personal digital assistant, an electronic pager, and a digital watch. In an illustrative example, information is transmitted in the form of e-mail. Further, a computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system.

While the invention has been described by illustrative embodiments, additional advantages and modifications will occur to those skilled in the art. Therefore the invention in its broader aspects is not limited to specific details shown and described herein. Modifications may be made without departing from the spirit and scope of the invention. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments but be interpreted within the full spirit and scope of the appended claims and their equivalents.

[I / We] claim:

1. A port blocking method for securing data comprising:

a port request detection step of detecting a port request for use of a port sent by a process;

a process identification step of determining the identity of said requesting process;

a process check step of determining if said process should be permitted to access said port; and

a permit/deny step of allowing said port request to be fulfilled if said process should be permitted to access said port and denying said port request if said process should not be permitted to access said port.

2. The method of claim 1 where said process check step comprises:

a secure process list check step of determining whether said process appears on a list of secure processes.

3. A port blocking method for securing data comprising:

a port request detection step of detecting a port request for use of a port sent by a process;

an open port process identification step of, if said port request is an open port request, determining the identity of said requesting process;

an open port process check step of, if said port request is an open port request, determining if said process should be permitted to open said port;

an open port permit/deny step of, if said port request is an open port request, allowing said open port request to be fulfilled and tracking said open port request if said process should be permitted to open said port and denying said port request if said process should not be permitted to open said port;

a close port process completion step of, if said port request is a close port request, completing said port request; and

a close port logging step of, if said port request is a close port request, logging the closing of said port.

4. The method of claim 3 where said open port process check step comprises:

a secure process list check step of determining whether said process appears on a list of secure processes.

5. The method of claim 3 where said tracking of said open port request comprises keeping a log of process ID and returned port handle for said open port request, and said close port logging step of tracking the closing of said port comprises removing from said log said record of process ID and returned port handle for that port close request.

6. The method of claim 5 further comprising:

a security check step comprising the steps of checking whether a process has open ports, and denying security clearance for a process with open ports, and allowing security clearance for a process with no open ports.

7. The method of claim 6 where said open port process check step of comprises determining if said process identity appears on a secured process list, and where said step of allowing security clearance for a process with no open ports comprises the step of placing said process on said secured process list.

8. A port blocking system wherein said port blocking system operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

9. A port blocking system wherein said port blocking system operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port

request; and if said port request is a close port request, log the closing of said port.

10. A secured data transmission system having a port blocking system which operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

11. A secured data transmission system having a port blocking system which operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port request; and if said port request is a close port request, log the closing of said port.

12. A computer comprising a communications port and configured to protect secure data by including a port blocking system which operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

13. A computer comprising a communications port and configured to protect secure data by including a port blocking system which operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port request; and if

said port request is a close port request, log the closing of said port.

14. A computer-readable medium programmed to protect secure data by implementing a port blocking system which operates to detect a port request for use of a port sent by a process; determine the identity of said requesting process; determine if said process should be permitted to access said port; and allow said port request to be fulfilled if said process should be permitted to access said port and deny said port request if said process should not be permitted to access said port.

15. A computer-readable medium programmed to protect secure data by implementing a port blocking system which operates to operates to detect a port request for use of a port sent by a process; if said port request is an open port request, determine the identity of said requesting process; if said port request is an open port request, determine if said process should be permitted to open said port; if said port request is an open port request, allow said open port request to be fulfilled, track said open port request if said process should be permitted to open said port, and deny said port request if said process should not be permitted to open said port; if said port request is a close port request, complete said port request; and if said port request is a close port request, log the closing of said port.

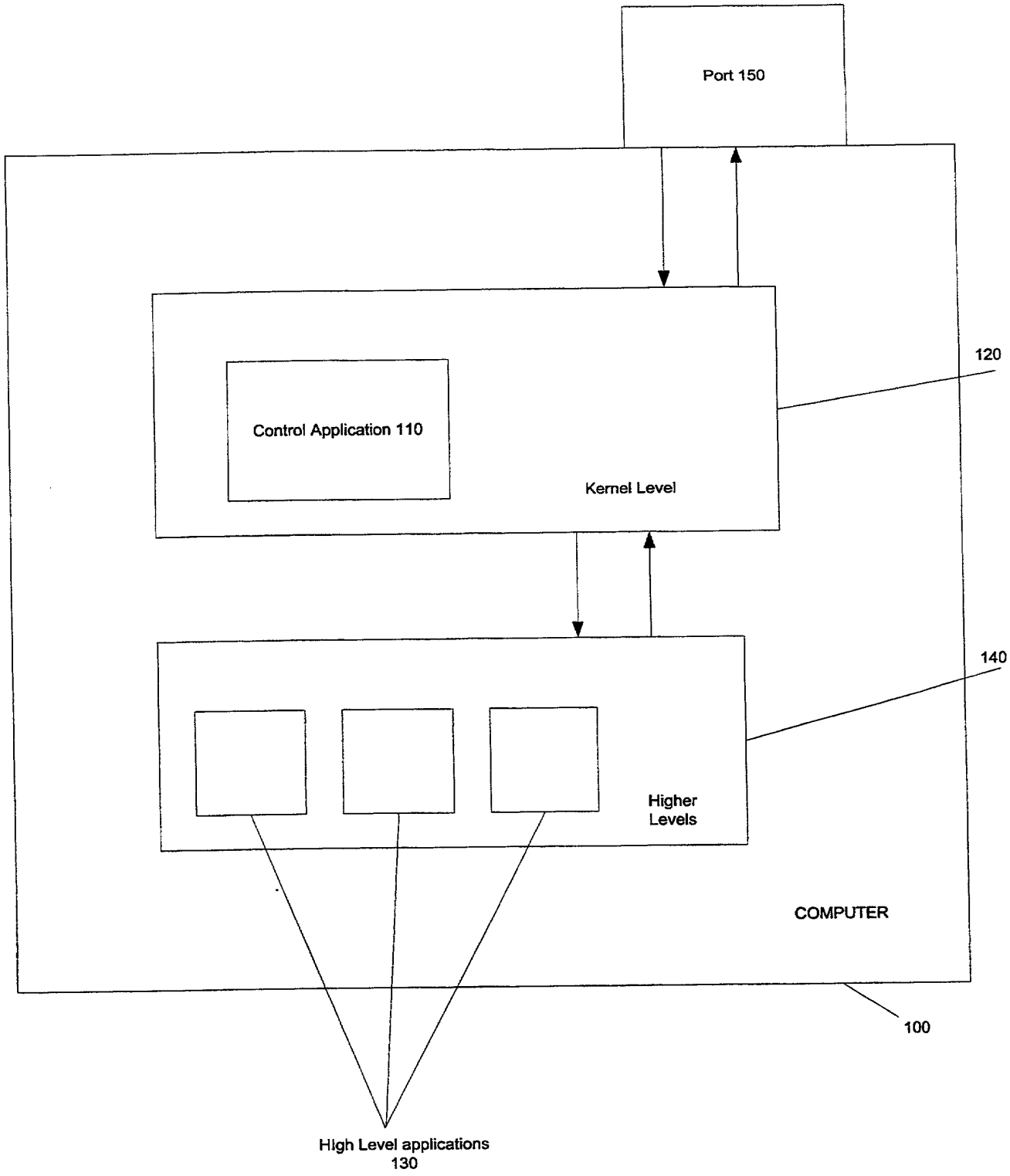
Port 150
Control Application 110
Kernel Level
120
140
Higher Levels
COMPUTER
100
High Level applications 130

FIG. 1

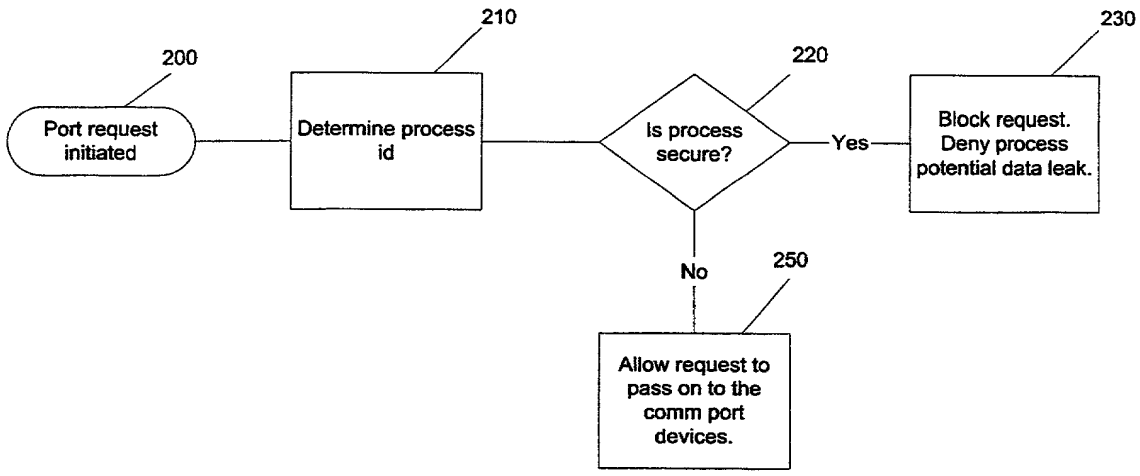
200
Port request initiated
210
Determine process id
220
Is process secure?
Yes
230
Block request. Deny process potential data leak.
No
250
Allow request to pass on to the comm port devices.

FIG. 2

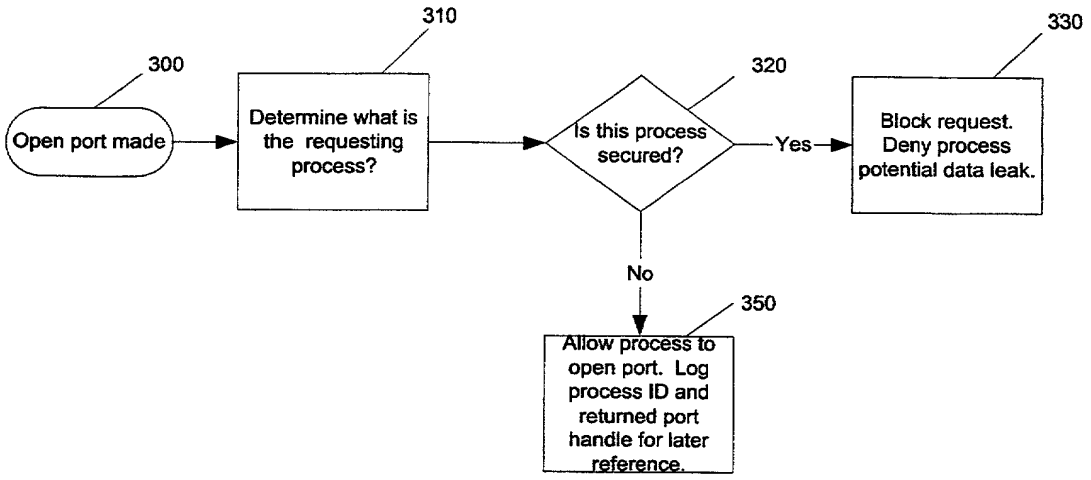

FIG. 3a

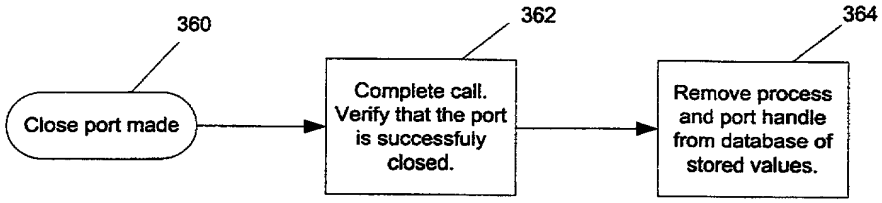

FIG. 3b

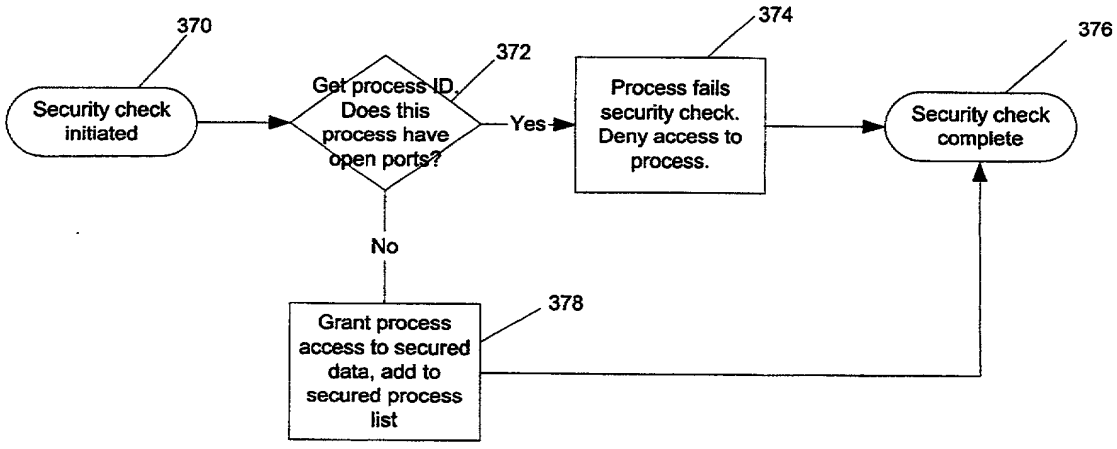

FIG. 3c

Doc. No. 1242-00

Declaration and Power of Attorney for Patent Application

As the below named inventor, we hereby declare that:

Our residence, post office address and citizenship are as stated next to our names,

We believe we are the original and first inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled PORT BLOCKING METHOD AND SYSTEM the specification of which is filed herewith.

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of the application:

PCT/US00/26839	9/29/00	pending
(Application Serial No.)	(Filing Date)	(Status) (patent, pending, abandoned)

We hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

T. Daniel Christenbury	Reg. No. 31,750
Guy T. Donatiello	Reg. No. 33,167
Paul A. Taufer	Reg. No. 35,703
Austin R. Miller	Reg. No. 16,602
James A. Drobile	Reg. No. 19,690
Gerard J. Weiser	Reg. No. 19,763
Robert A. McKinley	Reg. No. 43,793
Michael A. Patané	Reg. No. 42,982
Joan T. Kluger	Reg. No. 38,940
Sharon Fenick	Reg. No. 45,269
Stewart M. Wiener	Reg. No. 46,201
Armando A. Flores	Reg. No. 41,754
Felicity Rowe	Reg. No. 47,042

13

Address all telephone calls to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103 (215) 751-2475.

Address all correspondence to Paul A. Taufer, Schnader Harrison Segal & Lewis LLP, Suite 3600, 1600 Market Street, Philadelphia, PA 19103.

We hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

1 of 2

Full name of first and joint inventor: George Friedman

Inventor signature _____ 11/15/2000 Date

Residence: 7109 Montana Norte, Austin, Texas 78727 TX
Citizenship: USA
Mailing Address: same as above

2 of 2

Full name of second and joint inventor: Robert Phillip Starek

Inventor signature Robt P. Starek 11/15/2000 Date

Residence: 1807 W. Slaughter Lane #200-482, Austin, Texas 78748
Citizenship: USA
Mailing Address: same as above

Full name of third and joint inventor: Carlos A. Murdock

Inventor signature _____ 11/15/2000
Date

Residence: 4517 Avenue F, Austin, Texas 78751
Citizenship: USA
Mailing Address: same as above